IN THE CLAIMS

Please amend the claims as follows. Added text is underlined and deleted text is either struck through or shown in double enclosing brackets. Applicants aver that no new matter has been added.

1. (Currently Amended) A method ~~to detect~~ of detecting a fraudulent ~~activities~~ activity at a network-based transaction facility, the method comprising:

~~causing~~ generating a first identifier associated with a first user identity, the first identifier to be stored in a shill cookie on a client machine of the first user, the first identifier being generated responsive to at least a first of a ~~first sales-related~~ plurality of triggering events ~~event~~ with respect to the network-based transaction facility, the network-based transaction facility being coupled to ~~and initiated under the first user identity from~~ the client machine ~~which is coupled to the network-based transaction facility~~ via a network;

[[and]]

generating a second identifier associated with a second user identity, the second user identity to be stored in the shill cookie on the client machine, the second identifier being generated responsive to at least a second of the plurality of triggering events with respect to the network-based transaction facility;

receiving information stored on the shill cookie at the network-based transaction facility; and

detecting a potentially fraudulent activity by detecting a lack of correspondence between the first identifier ~~stored on the machine~~ and [[a]] the second identifier ~~associated with a second user identity responsive to a second sales-related event with respect to the network-based transaction facility and initiated under the second user identity from the machine~~.

2. – 4. (Canceled)

5. (Currently Amended) [[A]] The method of [[as in]] claim [[4]] 1, further comprising recording [[of]] the potentially fraudulent activity at the network-based transaction facility responsive to a detection of the lack of correspondence between the first identifier and the second identifier.

6. (Currently Amended) [[A]] The method of [[as in]] claim [[5]] 1, wherein the ~~second sales-related event~~ at least one of the plurality of triggering events is a sales transaction event, the method further comprising prohibiting a completion of the sales transaction event responsive to the detection of the lack of correspondence between the first identifier and the second identifier.

7. – 8. (Canceled)

9. (Currently Amended) [[A]] The method of [[as in]] claim [[8]] 1, wherein the ~~first sales-related event~~ at least one of the plurality of triggering events is a sales transaction event, the sales transaction event ~~includes~~ including at least one of registering with the network-based transaction facility, communicating an offer to sell an offering via the network-based transaction facility, communicating and offering to purchase the offering via the network-based transaction facility, communicating a feedback regarding a transaction, [[and]] or updating a profile maintained by the network-based transaction facility.

10. (Canceled)

11. (Currently Amended) [[A]] The method of [[as in]] claim [[10]] 1, further comprising:

~~causing the first identifier and the second identifier to be stored on the machine with a shill cookie;~~

causing a cookie identifier to be stored with the shill cookie;

causing the shill cookie to be coupled to a cookie bundle [[which]] that records a plurality of transaction preferences for the fist user identity and the second user identity on the client machine;

causing the shill cookie bundle to be sent from the client machine to the network-based transaction facility when the second user identify makes the ~~second sales transaction event~~ the at least the second of the plurality of triggering events with the network-based transaction facility using the client machine;

~~causing the shill cookie to be appended with the second identifier responsive to the detection of the lack of correspondence between the first identifier and the second identifier at one of the machine and the network-based transaction facility;~~

causing the cookie bundle to be inspected for the potentially fraudulent activity; and

causing the potentially fraudulent activity to be recorded into a database.

12. (Currently Amended) [[A]] The method of [[as in]] claim [[11]] 11, wherein an inspection of the shill cookie comprises a source for the detection of the lack of correspondence between the first identifier and the second identifier.

13. (Currently Amended) [[A]] The method of [[as in]] claim [[12]] 1, further comprising [[:]]

causing the shill cookie ~~bundle~~ to be a non-session cookie residing on the client machine for a predetermined amount of time.

14. (Currently Amended) [[A]] The method of [[as in]] claim [[13]] 1, further comprising [[:]] causing the shill cookie to be appended every time a new user identifier is used to establish a [[new]] third of the plurality of triggering events ~~event~~ with the network-based transaction facility using the client machine wherein there is a lack of correspondence between the new user identifier and the first user identifier.

15. (Canceled)

16. (Currently Amended) [[A]] The method of [[as in]] claim [[15]] 1, wherein the network-based transaction facility comprises an Internet-based auction facility.

17. (Currently Amended) [[A]] The method of [[as in]] claim [[16]] 1, further comprising [[:]] causing the shill cookie to record and to store a predetermined number of user identifiers.

18. (Currently Amended) [[A]] The method of [[as in]] claim [[17]] 1, further comprising causing the shill cookie ~~and the cookie bundle~~ to be encoded ~~such that the shill cookie and the bundle cookie are coded~~.

19. (Currently Amended) [[A]] The method of [[as in]] claim [[18]] 1, further comprising causing the shill cookie ~~and the cookie bundle~~ to be encrypted.

20. (Currently Amended) [[A]] The method of [[as in]] claim [[19]] 1, further comprising:
generating a potential fraudulent activities table having a fraudulent activity field, a cookie identifier field, a user identifier field, and a frequency field;
recording each of [[the]] a plurality of potentially fraudulent activities and corresponding information into the potential fraudulent activities table;
updating the potential fraudulent activities table at least on a periodic basis; and
providing an updated report of the potential fraudulent activities table to an investigation [[team]] team.

21. (Currently Amended) [[A]] The method of [[as in]] claim [[20]] 20, further comprising [[:]] configuring the potential fraudulent activities table to include a transaction product category field, a transaction country field, a transaction price range field, and a transaction activity field.

22. – 23. (Canceled)

24. (Currently Amended) [[A]] The method of [[as in]] claim [[20]] 20, further comprising providing the network-based transaction facility with a capability ~~to override~~ of overriding the updated report to the investigation team ~~as necessary~~.

25. (Currently Amended) [[A]] The method of [[as in]] claim [[24]] 1, further comprising providing a priority ranking system having a low priority for a low potential fraudulent activity frequency, a medium priority for a medium potential fraudulent activity ~~frequency~~ frequency, and a high priority for a high potential fraudulent activity frequency.

26. (Canceled)

27. (Currently Amended) [[A]] The method of [[as in]] claim [[26]] 1, wherein the potentially fraudulent activity includes at least one of shill biddings and shill feedbacks.

28. (Canceled)

29. (Currently Amended) [[A]] The method of [[as in]] claim [[28]] 1, further comprising causing the detection of the potentially fraudulent activity responsive to a matching of ~~at least two~~ a plurality of user transaction preferences from ~~at least two~~ a plurality of different user identifies.

30. (Currently Amended) [[A]] The method of [[as in]] claim [[29]] 29, wherein the plurality of user transaction preferences ~~comprise~~ include credit card numbers, bidding histories, payment methods, and shipping addresses.

31. (Currently Amended) A non-transitory computer readable storage medium comprising instructions, which when executed on a processor, cause the processor to perform a method [[for]] of detecting suspicious transactions made over a network-based transaction facility using a client machine, the method comprising:

~~causing~~ generating a first identifier associated with a first user identity, the first identifier to be stored in a shill cookie on a client machine of the first user, the first identifier being generated responsive to at least a first of a ~~first sales-related~~ plurality of triggering events ~~event~~ with respect to the network-based transaction facility, the network-based transaction facility being coupled to ~~and initiated under the first user identity from~~ the client machine ~~which is coupled to the network-based transaction facility~~ via a network; [[and]]

generating a second identifier associated with a second user identity, the second user identity to be stored in the shill cookie on the client machine, the second identifier being generated responsive to at least a second of the plurality of triggering events with respect to the network-based transaction facility;

transmitting information stored on the shill cookie to the network-based transaction facility; and

detecting a potentially fraudulent activity by detecting a lack of correspondence between the first identifier ~~stored on the machine~~ and [[a]] the second identifier ~~associated with a second user identity responsive to a second sales-related event with respect to the network-based transaction facility and initiated under the second user identity from the machine~~.

32. (Canceled)

33. (Currently Amended) A system to detect a fraudulent ~~activities~~ activity at a network-based transaction facility, the system comprising:

an identifier processor to ~~cause a first identifier associated with a first user identity to~~ generate and forward a shill cookie over a network to be stored on a client machine responsive to ~~a first sales-related event~~ at least a first of a plurality of triggering events being produced at the client machine after the client machine accesses the network-based transaction facility via the network , the shill cookie to contain information related to a first identifier associated with a first user identity, ~~with respect to the network-based transaction facility and initiated under the first user identity from the machine which is coupled to the network-based transaction facility via a network~~; the identifier processor further to generate a second identifier associated with a second user identity, the second user identity to be stored in the shill cookie on the client machine, the second identifier being generated responsive to at least a second of the plurality of triggering events with respect to the network-based transaction facility; and

a [[first]] detection processor to detect a potentially fraudulent activity by detecting a lack of correspondence between the first identifier ~~stored on the machine~~ and [[a]] the second identifier ~~associated with a second user identity responsive to a second sales-related event with respect to the network-based transaction facility and initiated under the second user identity from the machine~~.

34. (Canceled)

35. (Currently Amended) [[A]] The system [[as in]] of claim [[34]] 33, wherein the ~~said second~~ detection processor is to receive from the client machine both the first identifier and the second identifier at the network-based transaction facility ~~from the machine, and to detect the lack of correspondence between the first identifier and second identifier at the network-based transaction facility~~.

36. (Currently Amended) [[A]] The system [[as in]] of claim [[35]] 33, further comprising a [[first]] recording processor to record the potentially fraudulent activity at the network-based transaction facility responsive to [[a]] the detection of the lack of correspondence between the first identifier and the second identifier.

37. (Currently Amended) [[A]] The system [[as in]] of claim [[36]] 33, further comprising a cookie recording processor to record the first identifier and the second identifier to be recorded within [[a]] the shill cookie.

38. (Currently Amended) [[A]] The system [[as in]] of claim [[37]] 33, further comprising:

~~a storing processor to cause the first identifier and the second identifier to be stored on the machine within a shill cookie and a cookie identifier to be stored within the shill cookie;~~

a bundling processor to cause the shill cookie to be coupled to a cookie bundle [[which]] that records a plurality of transaction preferences for the first user identity and the second user identity on the client machine;

a sending processor to cause the shill cookie bundle to be sent from the client machine to the network-based transaction facility when the second user identify makes the ~~second sales transaction event~~ at least the second of the plurality of triggering events with the network-based transaction facility using the client machine;

an appending processor to cause the shill cookie to be appended with the second identifier responsive to the detection of the lack of correspondence between the first identifier and the second identifier at one of the client machine and the network-based transaction facility;

an inspection processor to cause the cookie bundle to be inspected for the potentially fraudulent activity; and

a [[second]] recording processor to cause the potentially fraudulent activity to be recorded into a database.

39. (Currently Amended) [[A]] The system [[as in]] of claim [[38]] 33, further comprising:

a tabulating processor to generate a potential fraudulent activities table having a fraudulent activity field, a cookie identifier field, a user identifier field, and a frequency field;

a [[third]] recording processor to record each of [[the]] a plurality of potentially fraudulent activities and corresponding information into the potential fraudulent activities table; and

an updating processor to update the potential fraudulent activities table at least on a periodic basis and to provide an updated report of the potential fraudulent activities table to an investigation team.

40. (Canceled)